IT Service Continuity:

Achieving Embeddedness Through Planning

Marko Niemimaa
Turku Centre for Computer Science
Turku School of Economics, University of Turku
Turku, Finland
e-mail: mailni@utu.fi

Jonna Järveläinen
Information Systems Science
Turku School of Economics, University of Turku
Turku, Finland
e-mail: jonna.jarvelainen@utu.fi

***Abstract*— Business customers and regulations as well as different IT service management frameworks expect that IT services are continuously operating. A service interruption might have severe impact on customer relationships, business, sales or image of the company. Therefore, organisations spend enormous amounts of time in continuity and recovery planning for IT services, and several continuity planning methodologies have been introduced. However, the connection between continuity planning and continuity management is somewhat unclear, and embedding the continuity practices into organisations have not been discussed in detail in planning methodologies. This paper will focus on how IT service continuity planning embeds continuity by reviewing continuity planning methods. The continuity planning practices that influence achieving embeddedness are analysed from qualitative and quantitative data from large organisations operating in Finland. The findings suggest that a number of planning practices support the transition from planning to embeddedness, such as creating awareness, increasing commitment, integrating the continuity practices into organisational processes and learning from incidents.**

Keywords- IT service continuity, continuity planning, continuity management, embeddedness

I. INTRODUCTION

Ticket sales in Finnish movie theatres interrupted in the autumn 2012, because the raging hurricane Sandy on the west coast of the US caused an incident on an IT service platform [1]. Several pharmacies and cities including Stockholm faced a similar surprise in November 2011, when IT services delivered by a large Nordic provider were interrupted due to a technical reason [2].

Business customers and regulations as well as different service management frameworks expect that IT services operate continuously; a service interruption might have severe impact on customer relationships, business, sales or image of the company. Disruption on the ability to operate IT services, can have even wider consequences, potentially affecting the whole society. Therefore, most organisations spend enormous amounts of time in continuity and recovery planning for IT services – both internal and outsourced – and several continuity planning methodologies have been introduced [3]–[7].

However, the plans have to be implemented and the continuity practices presented in the plans introduced and embedded into the organisation before business benefits are achieved. Continuity planning literature covers these steps quite simplistically: plans have to be implemented, trained and regularly maintained as well as tested. Still, even the most meticulous plans might be useless when an incident happens during unusual circumstances, if employees do not recognise the potential crisis. Continuity management studies suggest that embeddedness decreases the business impacts of a service disruption [8], [9]. According to Herbane et al. [8] transition from planning to embeddedness is achieved over time as planned continuity practices become part of operational processes and individuals and groups are committed to pursuing continuous operations. At each phase of the planning process opportunities for transition to embeddedness exists [10] However, despite the recognised significance of embeddedness and the potential at each stage of planning process for realising the transition, how the planning process influences the transition to embeddedness has not been studied.

Therefore this paper analyses each phase of continuity planning process in IT service context and the organisational activities that may influence the transition to embeddedness. In order to increase understanding on the transition, we will review continuity planning methods and analyse empirical data. The data on continuity planning has been gathered using qualitative interviews and a quantitative survey from private and public organisations operating in Finland.

The empirical findings suggest, instead of unidirectional relation (from planning to embeddedness), a bidirectional relation exists between continuity planning and embeddedness. Further, qualitative differences in organisational activities at each step of continuity planning influence achieving embeddedness.

First we describe continuity planning methodologies and search for activities, which might embed the practices into organisational processes and increase the commitment of employees. After presenting the methodology, we analyse the empirical data to find the evidence of embeddedness from the planning phases. Lastly we present the conclusions.

II. IT SERVICE CONTINUITY

Complexity of IT services makes delivering the services often risky. Risk management of IT services is identified as one of the major literature streams in service oriented literature [11]. Organisations try to avoid business losses by analysing IT risks but also by improving the continuity of services [8], [12].

IT service continuity (ITSC) management is concerned ‘with managing an organisation’s ability to continue

providing a pre-determined and agreed level of IT services to support the minimum business requirements following an interruption to the business' [13]. Scholars interested in ITSC have approached the topic from various perspectives in order to understand how to minimise the business impact of service interruptions as small disruption can cause costly delays, and longer ones demise an organisation [14].

Wan [13] argues ITSC planning needs to be integrated with IT service governance frameworks. By adopting the continuity planning processes as a part of service impact analysis it is possible to realise the dependencies amongst business services and the underlying IT components. In a similar manner, Bajgoric et al. [15] studied the relation between continuity planning and IT service management. They argued that prior literature has viewed continuity management either from technological or planning perspective and neglected the governance perspective. The authors argued, by integrating IT service management models (such as ITIL) with continuous computing infrastructure [16] substantial risk reduction and reduced service downtime can follow.

ITSC is a part of wider continuity management literature [13], [14] which aims to address all sources of disruptions [8]. The continuity management approaches represent the next generation of continuity planning [17]. Continuity planning (also known as Business Continuity Planning (BCP) emphasises the implementation of thorough plans that describe steps that govern recovery actions, focusing on the anticipation of failures [8]. Although continuity management also incorporates the stages of planning [8], continuity management emphasises achieving embeddedness. Embeddedness aims to improve flexibility, creativity and adaptability of the organisation when responding to disruptions [8], [18]. Employee commitment to continuity process [8], ongoing programme of education, awareness and training [19] as well as testing and exercising [20] have been suggested as activities to influence the transition from planning to embeddedness.

In the current literature, continuity methodologies have received more attention than continuity management. In order to integrate these discussions, understanding how the continuity methodologies relate to and influence the transition to embeddedness is needed.

III. THEORETICAL FRAMEWORK

In order to develop the theoretical framework for the study, we review three continuity planning methodologies and prior literature on embeddedness to understand the relation between the stages of continuity planning and achieving embeddedness. We chose the three as 1) all three methodologies are from IS scholars; 2) the authors are well-known continuity planning scholars; 3) the methodologies cover all stages common to most continuity planning methodologies [21] instead of focusing only on some. Six common continuity planning stages are used to structure the selected methodologies and discussion. Figure 1 illustrates the relation between continuity planning and embeddedness as uncovered from literature.

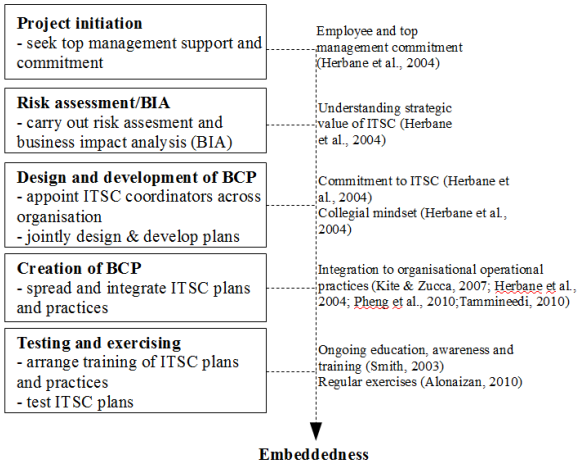

Figure 1 Relation between continuity planning and embeddedness.

Each step and their respective content is briefly reviewed next.

A. *Project initiation*

The project initiation phase aims at top management commitment and scoping of the planning project [21]. As stated by Botha and von Solms [3] '[i]t is imperative that management commitment is obtained' (p. 334) before the continuity planning proceeds. The top management commitment ensures proper allocation of resources for the project. Senior management participation gets them involved in the planning process and later to continuous process of development and maintenance of continuity plans (Ibid.). In addition, selected employees and customers should be informed of the project initiation [4] affecting employee commitment. Senior management and employee involvement and commitment influences the transition from planning to embeddedness [8].

B. *Risk assessment/Business Impact Analysis*

Risk assessments and especially business impact analysis is central to business continuity planning [7]. Where Gibb and Buchanan [4] suggest an approach that is more risk based approach, Botha and von Solms [3] suggest BIA and Lindström et al. [5] utilise both. Risk based approach focuses on identifying risks that threaten the organisation (or the part of it which is part of the scope) and assessing those risks [4]. BIA on the other hand, focuses on the outcome of those risks, for instance the on business impact of unavailability of IT services. BIA provides a common language for business and IT employees; organisation becomes aware of the continuity and understands what services have to be protected to minimise the business impacts of IT incidents. BIA facilitates discussion around the strategic value of IT services by utilising workshops and roundtable discussions with heterogeneous organisational groups to determine the costs associated with an IT service disruption, resulting in a prioritisation of organisational IT services [22]. Organisational understanding about the strategic value of ITSC planning increases as the continuity planning's relation to recovery speed becomes more explicit [8].

C. Design and development of BCP

At the next phase of the methodology, Lindström et al. [5] suggest the development of a continuity plan and implementation of a continuous maintenance process/plan. The process specific routine level plans should be detailed enough so that in an event of crisis another employee should be able to perform the tasks on behalf of another employee whose duty the task would normally be (Ibid.). To prepare the plans, Botha and von Solms [3] suggest identifying various scenarios in order to identify strategies for ensuring continuity and recovery of operations should a disruption realise. Preparing continuity plans is achieved by distributing responsibility across organisational departments, and appointing 'coordinators' whose task should be the management and development of the plans [23]. Joint development of the plans is likely to increase collegial mindset and commitment that influences the transition to embeddedness [8].

D. Creation of BCP

The creation of BCP phase creates detailed functional plans for each of the strategies identified at previous step that aim for the continuous operation of IT services [3]. The functional plans thus prepare the organisation to respond to the various identified scenarios, and thus closely resemble the process specific routines in Lindström et al. [5]. They instead see the implementation as a step where the 'implementation spans that the organisation starts to use the business continuity plan' (p. 249) and chosen risk mitigation measures are put in place.

Gibb and Buchanan [4] see that the purpose of the implementation phase is to introduce the changes to the organisation. This means 'putting in place any improvements to operating procedures, infrastructure, security, etc.' [4] that help the organisation to prepare for the risks threatening IT services. In addition, the implementation phase should also integrate the continuity practices to systems development life cycle. Integrating and spreading ITSC practices into operational practices, influences the transition to embeddedness [24].

E. Testing and exercising

In the testing phase, the continuity plans for IT services are tested. Unlike Lindström et al. [5] and Botha and von Solms [3], Gibb and Buchanan [4], address the testing, education and training phases extensively. Regularly and comprehensively testing the plans verifies whether the plans are still up to date (Ibid.). The testing phase can utilise either desk-based testing, technology oriented testing or process/service oriented testing (Ibid.). The purpose of the tests is to test the plans', technologies', and readiness of services to face the anticipated threats.

Organisations should ensure that the benefits and objectives of continuity planning have been communicated to the employees and further ensure the set objectives are achieved; this is to have education and training (Ibid.). The training and education should include the current employees as well as all new employees. Re-orientation trainings for the employees should be arranged every 6-12 months or when new procedures and systems are implemented (Ibid.). The ongoing programme of education, awareness and training as well as exercises establishes embeddedness [19], [25].

F. Maintenance and updating

Purpose of the maintenance and updating phase is to ensure that the continuity plans are responsive to changes in business environment [4]. Without maintenance and updating the plans drift apart from organisation as the organisation evolves through time and space. Asking questions such as 1) is the continuity documentation effective and current; 2) is the project sponsor committed; and 3) are the employees aware of their responsibilities and roles, assists the programme manager in the review (Ibid.).

For Lindström et al. [5], the maintenance phase is a start-up phase for a separate maintenance process, developed simultaneously with the plans. The structure, organisation and content of the maintenance process are left to lesser attention, but it can be assumed to resemble that of the actual BCP plan creation process. The regular maintenance of plans influences the transition to embeddedness [25].

As the review suggests, the planning methodologies include steps that seek management and employee commitment, employee involvement to continuity planning, the integration of practices to work routines and processes as well as educating employees on continuity practices. Indeed, this is what Herbane et al. [8] call embeddedness: continuity management is then not merely 'a plan' but constitutes the organisational processes of leadership, commitment which may be seen operating at individual and group levels' [8].

IV. Methodology

In this study, we use qualitative interviews [26], quantitative survey and two researchers to analyse the data in order to triangulate [27]. We chose these methods in order to increase understanding on how IT service continuity planning influences the transition to embedded practices.

In 2010, we conducted 18 qualitative interviews in large private organisations (by definition of Official Statistics of Finland [28]) employing more than 250 persons. Instead of randomly picking the organisations, we applied maximum variation purposeful sampling [29]. We contacted appr. 60 companies to find the interviewees, of which 18 were selected based on their willingness and schedule as well as variation. The number of interviews was guided by the principle of interviewing as many as was needed to find out what we needed to know, instead of statistical generalisation [26]. Semi-structured interviews of 45-60 minutes were conducted. The questions were based on the business continuity management framework presented by Herbane et al. [8], and we used the interviewing techniques of Myers & Newman [30] and adapted the questions based on the interviewee. The interviews were in IT (3 interviewees), service (6), insurance/banking (4) and manufacturing sectors (5). The companies employed 250 – 24.000 employees, and interviewed persons were CIOs or I(C)T managers (8), CISO or other security related managers (10) and others managers or experts (3). In most of the companies only one manager was interviewed, but in three companies managers had also invited other experts or managers for the session.

The interviews were firstly coded with mindmapping software into categories (e.g. plans, preparedness etc.) and subcategories (e.g. project initiation, written plans etc.), and after several analysis iterations similar subcategories than in continuity planning methodologies were discovered. From the mindmap, similarities and differences were recognised and the similar or different transcribed texts were compared to interpret the text. The authors discussed their controversial interpretations to find a common agreement.

Based on the findings from the qualitative interviews, a quantitative survey was done in 2012. The survey items were developed based on prior literature [8], [31], [32] and it was pretested in two phases: first with academics and then with six CIOs. The target group was also large organisations (employing more than 250 persons), but this time we sent the survey to both public and private organisations. The CIOs or IT managers of all organisations, which had given the contact details in a public contact database, were e-mailed (in total 630). Of these e-mail addresses 617 were valid, and after two reminders we received 84 responses (13.6%). The low response rate is equal to other information security related surveys [33].

The respondent organisations were categorised in three sectors: Public sector (N= 31), manufacturing (22) and services (30). Only 9 organisations employed more than 6000 employees, 27 organisations employed less than 500 employees, 23 organisations had 501-1000 employees and 23 organisations had 1001-6000 employees. The small organisations had quite small turnovers (public organisations reported their annual funding), 30 organisations had less than 100 million euro turnover, 17 organisations had 101-200 M€, 18 organisations 201-700 M€ and 15 organisations had more than 700 M€. Most of the organisations (69) had less than 50 employees in their IT department, most (40) had outsourced none or less than one quarter out of their IT infrastructure or services.

The triangulation was used 'to capture a more complete, holistic, and contextual portrayal of the unit(s) under study' [34]. The questionnaire findings were used here to describe the situation in general in numerical terms, the interview findings to provide detailed information about planning phases and their relation to embeddedness and two researchers' independent interpretation of the data to surface multiple interpretations of the data. The research approach allowed new dimensions of the relation between continuity planning and embeddedness to emerge [34] (i.e., from unidirectional view to bidirectional view as discussed next).

V. Findings and Discussion

Prior research addressing embeddedness has viewed the relation to organisational continuity activities (e.g., awareness, training, etc) from a unidirectional, deterministic view; continuity activities lead to embeddedness. Such approaches largely assume the continuity planning begins on a tabula rasa; organisation without existing practices or understanding of and commitment to continuity thinking.

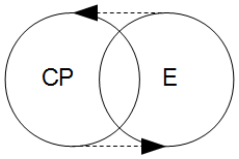

Figure 2. Relation between continuity planning (CP) and embeddedness (E).

However, the continuity planning begins and evolves in organisational context with its own historicity such that the existing practices and commitment to continuity planning influences the stages of planning. Embeddedness is thus not an end of continuity planning, but an active part of continuity planning itself, shaping and making the organisational planning activities. Figure 1 illustrates the relation in which the continuity planning (CP) is already influenced by a degree of embeddedness (E) and, on the other hand, the continuity planning influencing the degree of embeddedness.

Next, we provide a more detailed discussion to support our findings.

A. Project initiation

The continuity planning projects were initiated in the interviewed companies 1) after a major incident; 2) after customers had required it; 3) as a management initiative; or 4) as an IT or security experts' initiative. When organisation had experienced a major incident, some part of the company had learned a lesson. In these cases, the commitment and awareness of management as well as employees is clear and easily gained, and it is justifiable to engage into such project. Sometimes customers – new or existing ones – had either set continuity requirements for co-operation or asked whether the company complied with any IT service management framework or continuity standard. Fulfilling external requirements would lead to new customer acquisitions [8], and therefore business managers were willing to participate in the project. In some occasions, corporate headquarters or the top management initiated the continuity project and lower level managers and employees had no choice but to follow. Top management commitment was essential for success:

"A manager, who was about to retire, was responsible for [the planning project] and we managed to do the models and tools but then there was no energy to implement the project."

The most difficult situation for project initiation was when IT or security experts started it. The scope of the project was in danger of becoming too IT or security oriented and the commitment of business managers was hard to achieve. Sometimes IT department was not able to identify the business critical applications, the continuity of which would have been crucial. In this situation, the degree of embeddedness was low; continuity was not well embedded in the company. However, in the end, the essential top management support [3] was usually gained, influencing the degree of embeddedness.

The initiation of continuity planning suggests the degree of embeddedness shapes the initiation. Organisational experience, and customer requirements shaped the commitment of management, support and strategic thinking of continuity planning, suggesting a

degree of embeddedness had led to the initiation of continuity planning.

B. Risk assessment/Business Impact Analysis

According to our survey data, 76% of the organisations had done a thorough risk analysis for IT services, but only 44% of the respondents had done a systematic business impact analysis (BIA). Especially the public sector had not done a BIA, there was a statistically significant difference in means (public sector 2.64 and private sector 3.52, equal variances T= -3.253, p=0.02). The concept "business impact analysis" might be too forbidding for public organisations, since also the public sector had prioritised their IT systems mostly based on impacts on their customers.

The qualitative data gives us more details about this phase. BIA or risk assessments were conducted using interviews, questionnaires and discussions between business and IT service people. With interviews IT people have identified the most critical IT services for business and the costs business would be willing to pay for the continuity of a certain service. Other method for prioritising the services has been a questionnaire that has been sent to all business unit managers, who then provided prioritised lists of IT services that were then combined. A value chain analysis identifies the dependencies of IT services and business units, and forces business units to think about the "big picture" or the whole enterprise. This is a means to engage business and IT people in a joint effort for continuity [8].

We did not find any statistically significant differences between smaller and larger companies related to this planning phase. Nevertheless, according to our qualitative data the methods were different in smaller companies. They assessed risks by identifying the critical processes and then found the IT services required for the processes. The critical processes were discussed within the top management group and IT people then found the supporting systems and prioritised their continuity. In smaller companies, top management was merely used as an information source, sought for consultation to provide the needed information for IT experts in order to determine the most critical resources. The continuity mindset was not thus embraced in these companies, indicating a low degree of embeddedness.

C. Design and development of BCP

The design and development of continuity plans was often based on pre-filled planning templates with instructions how to use them.

"When I was recruited, my first task was to update the Company's IT system continuity plan […], a 150-200 pages long, monolithic and heavy document […]. We understood it would be irrational because the system range and complexity had increased, and the updating would take a long time and it would be 1000 pages long and obsolete when completed. So, I invented a 10 page the Principles of Continuity Planning document and a 3-page template."

The problem with the templates was in many organisations that business people did not understand how to fill them. They wrote the plans mechanically without thinking about whether they actually ensured continuity of IT services, the owners of which they were. Therefore the IT experts sometimes acted as continuity planning coordinators in some organisations, and either filled the templates with the business managers, trained them or discussed continuity issues with them. According to the survey data, these coordinators were used only in every fourth organisations. This was one way to decentralise planning and to distribute the continuity mindset outside the IT department and to create awareness and commitment increasing embeddedness. This emphasises the importance of training and discussion in order to achieve embeddedness.

In every second respondent organisation had decentralised planning to business units or departments. Plans were made on corporate, organisation, process and business unit level, but on information system level disaster recovery plans were more common. Crisis recovery teams, contact persons and key persons for recovery were named in the plans,, which reflects embeddedness, but also created commitment to continuity increasing embeddedness.

D. Creation of BCP

In two out of three organisations, business continuity was considered during the design of a new IT service. They had understood that if ITSC is integrated into the IT services in a later phase, costs would increase substantially. This suggests the continuity practices were embedded in processes.

However, according to our survey data, no organisation had a continuity plan for all processes (see Table 1). This finding might indicate that the whole organisations are not aware of continuity, since all the processes are not covered by the plans. As Wan [13] argues, if the continuity planning is part of service impact analysis, it is possible to understand the connection between business services (processes) and IT components supporting them. Our data suggests that IT and business service dependencies have not been fully realised in these companies.

According to our interviews, smaller companies considered the continuity plans too cumbersome to create and update, since the human resources were scarce. Thus the perceived lack resources may limit embeddedness. However, they used disaster recovery principles to apply in incidents and often tested back-up recoveries. The organisation had not realised the strategic role of continuity planning [8], suggesting low embeddedness.

E. Testing and exercising

Testing and exercising were discussed in the interviews but also survey data was gathered. Interview data suggests the testing of continuity plans was in some firms regular and in others rare, and some companies had had several incidents so extra testing was considered unnecessary.

TABLE I. PLANS IN ORGANISATIONS

Categories	**Plan Coverage (Frequencies)**				
	For all	***For all critical ones***	***For most critical ones***	***For some critical ones***	***For none***
BCP for processes		25	23	33	3
BCPs for IT	5	32	22	22	3
DRPs for IT	7	33	19	23	2
DR principles for IT	15	31	12	18	6

External audits by customers or third parties were very frequent in some firms although ITSC was not audited every time. Training for ITSC mostly concentrated on information security and not on continuity. In such cases, the degree of embeddedness had shaped the content and focus of the trainings and audit activities.

Few firms had initiated a yearly calendar, where every month a certain information system or part of infrastructure was tested with exercises; in March the Voice over Internet Protocol, in April the financial system etc. In this way, all parts of the organisation became aware of continuity on their turn since their operations were affected in some month of the year. Since the calendar was approximately the same or slightly altered every year, the exercising was routine like and embedded into the processes also in other departments than IT. However, in one large firm two security experts spent weeks for planning exercises and were doubtful whether this kind of regular testing would be applicable in their own firm due to scarce resources. According to our survey simulated tests or audits were not regular in public organisations. There was a statistically significant difference ($t=-2.848$, $p= 0.006$) between public (3.52) and private sector (2.77).

Almost all organisations (91.7%) did regular backups, but only two out of three tested data recovery from backups systematically according to our survey. One interviewee from a smaller company (650 employees) expressed the importance of these data recoveries:

"If something happens, and [the work of several weeks and persons] is lost, the costs are substantial. We perceive the backups and recovering from them really important [...]. We test it [backups] regularly and it has been documented so that it recoveries will be tested and they really are done."

F. Maintenance and updating

Interviewees from many organisations confirmed that regular updating of plans was part of their continuity practices (58.3% of survey respondents). Organisations had agreed continuity plans are updated regularly, e.g., every one or two years (documented on the plan) or after major incidents. When the maintenance schedule of the plan was agreed, it became part of a process, and thus embedded.

Interviewees shared a view that learning from mistakes was essential. Therefore, after major incidents the root cause was analysed and the ITSC plans updated to avoid the reoccurrence of the incident:

"After a bigger problem we make these final reports and otherwise document how the process has been done. When the root cause is found, we find a solution to avoid it happening again and check whether other locations need to be fixed too."

With this activity, IT department distributed the lessons learned to wider organisational audience and therefore kept continuity thinking alive. The importance of learning from mistakes has been mostly absent from the current literature. Ahmad et al. [35] have touched upon the topic and suggest incident reviews should not only focus on 'high-impact' incidents, but also review 'near misses' and 'high-learning' cases. The empirical findings provide further support for the significance of comprehensive incident reviews as learning from incidents is an activity that influences achieving embeddedness.

To summarise, the findings suggest that continuity planning process should emphasise awareness and commitment among employees as well as integration of continuity practices into organisational processes as activities at each stage of planning in order to realise the transition to embeddedness. Most interestingly, organisations understand learning from incidents as an important part of maintenance of plans, which has not been recognised in prior planning methodologies. Further, our findings suggest qualitative differences at each phase influences the transition. Achieving embeddedness is thus not a matter of what activities are carried out in as much as how the activities are carried out.

VI. CONCLUSIONS

IT service disruptions can have dramatic effects on organisations. Increased reliance on IT services requires attention to IT service continuity (ITSC). ITSC management is concerned with organisations ability to provide IT services that are operating as organisation expects.

This paper set out to study: how information service continuity planning embeds continuity into organisational practices? In order to increase understanding, the prior literature on ITSC and continuity planning was reviewed and data analysed. Findings suggest all ITSC planning phases potentially influence whether organisations can realise the transition from planning to embeddedness.

In the project initiation phase, management commitment influences transition to embeddedness, and implies a degree of embeddedness as management commitment. Project initiator influences the project scope. An ITSC project initiated by IT experts is likely to stay as an IT centric rather than organisation wide reflecting a low degree of embeddedness.

In risk assessment / BIA phase, organisations with higher embeddedness use BIA to gain the commitment and input of wider organisational community influencing embeddedness. In organisations with lower embeddedness, the top management was not actively involved in BIA but merely an information source limiting the continuity planning activities and the influence of activities on embeddedness.

Next in design and development phase, organisations with higher degrees of embeddedness appoint ITSC coordinators across business units that further influence organisational commitment. ITSC coordinators involvement to plan creation promotes collegial mindset influencing embeddedness. Documenting responsibilities in plans reflect a higher degree of embeddedness and promote employee commitment to ITSC influencing embeddedness.

After development, the plans are created. Then the impoverished view on the connection between IT services and business processes reflects weak embeddedness and limits the organisations strategic understanding about ITSC inhibiting gaining embeddedness. Perceived lack of organisational resources, for plan implementation may inhibit transition from recovery plans to embeddedness.

When plans are tested, the formal and periodic exercises that evaluate the integration of ITSC practices

into organisation support transition to embeddedness. The degree of embeddedness influences the extent to which continuity plans have been integrated into the organisation as well as the form and content of the exercises. Constant incidents may complement formal training and influence organisational commitment to ITSC influencing transition to embeddedness.

Lastly in the maintenance phase, scheduled maintenance requires commitment to ITSC, enhancing the transition from planning to embeddedness. Revising incidents and learning from mistakes increases organisational awareness by keeping continuity thinking alive. Organisations with higher degrees of embeddedness may also review the 'near misses' and 'high-learning' case.

Building on the findings we conclude that organisations should not merely see the planning process as a process for building ITSC plans but as an opportunity to realise, or at least start realising, the transition from planning to embeddedness. Not only what the organisation does, but how the organisation does it, i.e., how it evolves and shifts through the stages of a planning process, has potential to significantly influence the results and outcome of the ITSC planning process. Top management involvement, collegial continuity mindset, awareness on ITSC continuity, integrated ITSC practices and joint learning from incidents should be emphasised in any ITSC planning project. Transition to embeddedness is realised throughout the process of planning, not as a mere afterthought.

Research on continuity planning has largely suggested atheoretical ITSC practices for achieving the embeddedness. Future research on ITSC should provide approaches that have stronger a connection to theory that supports the transition to embeddedness. Further, as the current literature has not been explicit on how the awareness of employees or organisations differs from that of embeddedness, future research should study the relation of the two. Lastly, as the embeddedness is achieved through a process of transition empirical understanding how the process evolves over time is needed and how the degree of embeddedness could be measured.

REFERENCES

[1] Yle, "Sandy-myrsky sotkenut tietojärjestelmiä Suomessakin," Yle Uutiset, 30-Nov-2012.

[2] Myndigheten för samhällsskydd och beredskap, "Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter," MSB367, 2012.

[3] J. Botha and R. Von Solms, "A cyclic approach to business continuity planning," Inf. Manag. Comput. Secur., vol. 12, no. 4, pp. 328–337, 2004.

[4] F. Gibb and S. Buchanan, "A framework for business continuity management," Int. J. Inf. Manag., vol. 26, no. 2, pp. 128–141, 2006.

[5] J. Lindström, S. Samuelsson, and A. Hägerfors, "Business continuity planning methodology," Disaster Prev. Manag., vol. 19, no. 2, pp. 243–255, 2010.

[6] R. L. Tammineedi, "Business Continuity Management: A Standards-Based Approach," Inf. Secur. J. Glob. Perspect., vol. 19, no. 1, pp. 36–50, 2010.

[7] V. Cerullo and M. J. Cerullo, "Business Continuity Planning: A Comprehensive Approach," Inf. Syst. Manag., vol. 21, no. 3, pp. 70–78, 2004.

[8] B. Herbane, D. Elliott, and E. Swartz, "Business Continuity Management: time for a strategic role?," Long Range Plann., vol. 37, no. 5, pp. 435–457, Oct. 2004.

[9] J. Järveläinen, "IT incidents and business impacts: validating a framework for continuity management in information systems," Int. J. Inf. Manag., vol. in press, 2013.

[10] British Standard Institute, "BS25999-1:2006 - Business Continuity Management - Part 1: Code of Practice." British Standards Institute, 2006.

[11] H. Demirkan, R. J. Kauffman, J. A. Vayghan, H.-G. Fill, D. Karagiannis, and P. P. Maglio, "Service-oriented technology and management: Perspectives on research and practice for the coming decade," Electron. Commer. Res. Appl., vol. 7, no. 4, pp. 356–376, Winter 2008.

[12] H. Salmela, "Analysing business losses caused by information systems risk: a business process analysis approach," J. Inf. Technol., vol. 23, no. 3, pp. 185–202, 2008.

[13] S. Wan, "Service impact analysis using business continuity planning processes," Campus-Wide Inf. Syst., vol. 26, no. 1, pp. 20–42, 2009.

[14] B. Van de Walle and A. F. Rutkowski, "A fuzzy decision support system for IT service continuity threat assessment," Decis. Support Syst., vol. 42, no. 3, pp. 1931–1943, 2006.

[15] N. Bajgoric, M. Spremic, and L. Turulja, "Implementation of the IT governance standards through business continuity management: Cases from Croatia and Bosnia-Herzegovina," in *Proceedings of the 33rd International Conference on Information Technology Interfaces (ITI)*, 2011, pp. 43–50.

[16] N. Bajgoric and Y. B. Moon, "Enhancing systems integration by incorporating business continuity drivers," Ind. Manag. Data Syst., vol. 109, no. 1, pp. 74–97, Jan. 2009.

[17] B. Herbane, "The evolution of business continuity management: A historical review of practices and drivers," Bus. Hist., vol. 52, no. 6, pp. 978–1002, Oct. 2010.

[18] S. P. Low, J. Liu, and M. Kumaraswamy, "Institutional Compliance Framework and business continuity management in Mainland China, Hong Kong SAR and Singapore," Disaster Prev. Manag., vol. 19, no. 5, pp. 596–614, 2010.

[19] D. Smith, "Business continuity and crisis management," Manag. Q., pp. 27–33, 2003.

[20] D. Paton, "Business Continuity During and After Disaster: Building Resilience Through Continuity Planning and Management," Asbm J. Manag., vol. 2, no. 2, pp. 1–16, 2009.

[21] M. Pitt and S. Goyal, "Business continuity planning as a facilities management tool.," Facilities, vol. 22, no. 3/4, pp. 87–99, Mar. 2004.

[22] S. P. Foster and K. Dye, "Building continuity into strategy," J. Corp. Real Estate, vol. 7, no. 2, pp. 105–119, 2005.

[23] J. Moyer and K. Novick, "Introducing a New Resource for Water and Wastewater System Business Continuity Planning," Am. Water Works Assoc. J., vol. 104, no. 3, pp. 37–39, 2012.

[24] C. Kite and G. Zucca, "How to access your Board/C-suite and make an effective case for business continuity investments," J. Bus. Contin. Emerg. Plan., vol. 1, no. 4, pp. 332–339, 2007.

[25] A. Alonaizan, "Developing a business continuity programme at Arab National Bank.," J. Bus. Contin. Emerg. Plan., vol. 3, no. 3, pp. 216–221, May 2009.

[26] S. Kvale, InterViews. An introduction to qualitative research writing. Sage Publications, Thousand Oaks, CA, 1996.

[27] R. K. Yin, Case study research: Design and methods, vol. 5. Sage publications, INC, 1990.

[28] Official Statistics of Finland, "Finnish enterprises 2009 (e-publication)," Statistics Finland, Helsinki, Nov. 2010.

[29] M. Q. Patton, Qualitative research & evaluation methods. Sage Publications, Incorporated, 1990.

[30] M. D. Myers and M. Newman, "The qualitative interview in IS research: Examining the craft," Inf. Organ., vol. 17, no. 1, pp. 2–26, 2007.

[31] W. S. Chow and W. O. Ha, "Determinants of the critical success factor of disaster recovery planning for information systems," Inf. Manag. Comput. Secur., vol. 17, no. 3, pp. 248–275, Jul. 2009.

[32] J. Järveläinen, “Information security and business continuity management in interorganizational IT relationships,” Inf. Manag. Comput. Secur., vol. 20, no. 5, pp. 332–349, Nov. 2012.

[33] A. G. Kotulic and J. G. Clark, “Why there aren’t more information security research studies,” Inf. Manage., vol. 41, no. 5, pp. 597–607, May 2004.

[34] T. D. Jick, “Mixing Qualitative and Quantitative Methods: Triangulation in Action,” Adm. Sci. Q., vol. 24, no. 4, pp. 602–611, Dec. 1979.

[35] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, “Incident response teams – Challenges in supporting the organisational security function,” Comput. Secur., vol. 31, no. 5, pp. 643–652, Jul. 2012.

[36]